CLAIMS

What is claimed is:

1. *In a video device, a method comprising:*

continuously clocking a cipher unit, upon power on/reset, to introduce entropy into the cipher unit;

in response to a subsequent request after n clocks for a first pseudo random number, where n is an integer, taking a first plurality of output bits of the cipher unit and storing the first output bits;

upon storing the first output bits, outputting the stored first output bits as the first pseudo random number; and

transitioning to a selected one of the continuously clocking state, another output taking state, and an authenticated state depending on whether upon provision of the first pseudo random number, an indication of an unsuccessful authentication using the first pseudo random number, another request for a second pseudo random number, or an indication of a successful authentication using the first pseudo random number is received.

2. *The method of claim 1, wherein the method further comprises*

taking a second plurality of output bits of the cipher unit, while in said another output taking state, and storing the second output bits; and

upon storing the second output bits, outputting the stored second output bits as the second pseudo random number.

3. *The method of claim 1, wherein the method further comprises*

receiving another request for a third pseudo random number, while in said authenticated state;

transition to said another output taking state.

4. The method of claim 1, wherein the method further comprises

receiving a selected one of an unauthenticated notification and a detachment notification, while in said authenticated state; and

transition to said continuously clocking state.

5. A video apparatus comprising:

a cipher unit to generate a sequence of ciphering bits to cipher video to be transmitted by the video apparatus; and

a state machine coupled to the cipher unit to also use the ciphering unit to generate pseudo random numbers to authenticate video receiving devices attached to said video apparatus.

6. The video apparatus of claim 5, wherein the state machine is equipped to transition to a continuous clocking state, upon power on/reset, and causes the cipher unit to be continuously clocked to introduce entropy into the cipher unit.

7. The video apparatus of claim 6, wherein the state machine is further equipped to transition from said continuous clocking state to a first output taking state, in response to a subsequent request after n clocks for a first pseudo random number, where n is an integer, to take a first plurality of output bits of the cipher unit, and store the taken first output bits.

8. The video apparatus of claim 7, wherein the state machine is further equipped to transition from said first output taking state to an output state, upon storing the first output bits, to output the stored first output bits as the first pseudo random number.

9. The video apparatus of claim 8, wherein the state machine is further equipped to transition from said output state to a selected one of the continuously clocking state, a second output taking state, and an authenticated state depending on whether upon provision of the first pseudo random number, an indication of an unsuccessful authentication using the first pseudo random number, another request for a second pseudo random number, or an indication of a successful authentication using the first pseudo random number is received.

10. The video apparatus of claim 9, wherein the state machine is further equipped to transition from said second output taking state to said output state upon taking a second plurality of output bits of the cipher unit and storing the second output bits.

11. The video apparatus of claim 9, wherein the state machine is further equipped to transition from said authenticated state to said another output taking state upon receiving another request for a third pseudo random number.

12. The video apparatus of claim 9, wherein the state machine is further equipped to transition from said authenticated state to said continuously clocking state upon receiving a selected one of an unauthenticated notification and a detachment notification.

13. A pseudo random number generator comprising:

a cipher unit to generate a sequence of ciphering bits to cipher a stream of data; and

a state machine coupled to the cipher unit to also use the ciphering unit generate a plurality of pseudo random numbers based on selected ones of said cipher bits.

14. The pseudo random generator of claim 13, wherein the state machine operates in a selected one of a continuous clocking state, a first cipher bit taking state, an output state, a second cipher bit taking state, and an authenticated state, wherein the state machine causes the cipher unit to be continuously clocked while in said continuous clocking state to introduce entropy in said cipher unit, causes first and second plurality of said cipher bits to be taken and stored, in said first and second cipher bit taking states respectively, causes the stored first/second cipher bits to be output as first/second random numbers, causes the cipher bits of the cipher unit to be used to cipher said stream of data during said authenticated state.

15. The pseudo random generator of claim 14, wherein the state machine is equipped to transition from said continuous clocking state to said first output taking state, in response to a subsequent request after n clocks for said first pseudo random number, where n is an integer, and to transition from said first output taking state to said output state, upon storing the first output cipher bits.

16. The pseudo random generator of claim 14, wherein the state machine is equipped to transition from said output state to a selected one of the continuously *clocking state, the second output taking state, and the authenticated state depending on whether upon provision of the first pseudo random number, an indication of an unsuccessful authentication using the first pseudo random number, another request for a second pseudo random number, or an indication of a successful authentication using the first pseudo random number is received.*

17. The pseudo random generator of claim 14, wherein the state machine is equipped to transition from said second output taking state to said output state upon taking the second plurality of output cipher bits of the cipher unit and storing the second output cipher bits.

18. The pseudo random number generator of claim 14, wherein the state machine is further equipped to transition from said authenticated state to said second output taking state upon receiving another request for a third pseudo random number, and to said continuously clocking state upon receiving a selected one of an unauthenticated notification and a detachment notification.